# Cybersecurity Incident Report

| **Section 1: Identify the type of attack that may have caused this**  **network interruption** | |
| --- | --- |
| One potential explanation for the website's connection timeout error message is:  The log shows that the server was receiving a large number of TCP SYN requests from an unfamiliar ip address, overwhelming the server’s ability to respond to these requests. This scenario is characteristic of a SYN flood attack which is a type of Denial of service attack.  This event is likely a denial of service (DOS) SYN flood attack as a large amount of SYN requests came from only one IP address making it unlikely to be a DDOS attack.  However due to the amount of SYN requests it overwhelms to servers ability to fill requests and any attempt to visit the site will result in a connection timeout error. | |
|

| **Section 2: Explain how the attack is causing the website to malfunction** |
| --- |
| When website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. Explain the three steps of the handshake:   1. The client sends SYN packets to the server , indicating its intention to establish a connection 2. The server responds to the SYN attack acknowledging the client’s request and sending its own SYN sequence number. 3. The client sends an ACK packet to the server confirming the receipt of SYN ACK packet and therefore completing the three way handshake   In a SYN flood attack the attacker sends a large number of SYN packets to the server to abuse the TCP handshake process by not completing the third step of the three way handshake by sending the ACK packet and therefore consumes the servers allocated resources to keep track of the pending connection requests.  The logs will indicate that the web server was receiving a large number of TCP SYN requests from an unfamiliar IP address. Theses requests were not being followed through by a final ACK packet. As the number of incomplete connections grew the server resources become exhausted and results in the website being unresponsive. |
|  |